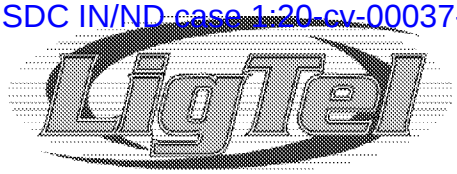
EXHIBIT 6



Cybersecurity Policies

Acceptable Use Polic	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 9

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.0 Purpose

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

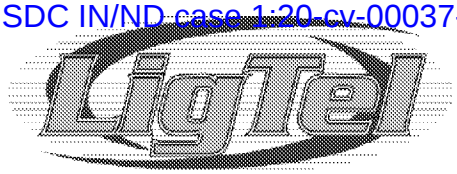
3.0 Scope

The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.

4.0 Policy

4.1 E-mail Use

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.



- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

- The user is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.

- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that detailed information about the use of email may be covered in the company's Email Policy.

4.2 Confidentiality

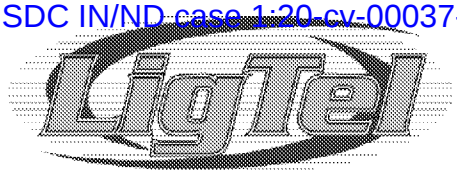
Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

4.3 Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use

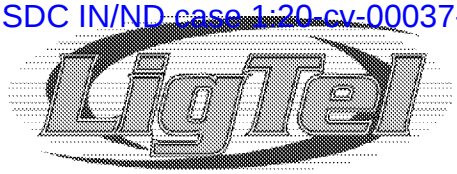
The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:



- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.5 Blogging and Social Networking

Blogging and social networking by the company's employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging is never allowed from the corporate computer network and using social networking is discouraged from the corporate computer network. In no blog or website, including blogs or sites published from personal or public systems, shall the company be identified, company business matters discussed, or material detrimental to the company published. The user must not identify himself or herself as an employee of the company in a blog. The user assumes all risks associated with blogging and/or social networking.



Acceptable Use Polic	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 9

4.6 Instant Messaging

Instant Messaging is allowed for corporate communications only. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

4.7 Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

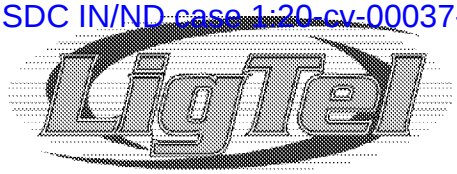
4.8 Web Browsing

The Internet is a network of interconnected computers of which the company has very little control. The employee should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Personal Use. The company recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

4.9 Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.



Cybersecurity Policies

4.10 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network unless specifically related to job function.

4.11 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

4.12 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.13 Bandwidth Usage

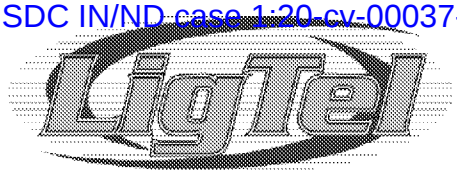
Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.

4.14 Personal Usage

Personal usage of company computer systems is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

4.15 Remote Desktop Access

Use of non-company-supplied remote desktop software and/or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited.



Acceptable Use Polic	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 6 of 9

4.16 Circumvention of Security

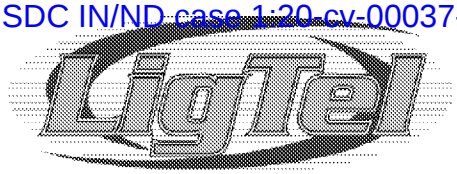
Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.



Acceptable Use Polic	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 7 of 9

4.18 Non-Company-Owned Equipment

Non-company-provided equipment is expressly prohibited on the company's corporate computer network.

4.19 Personal Storage Media

The company does not restrict the use of personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the corporate network, provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the company network. Use of personal storage media must conform to the company's Mobile Device Policy.

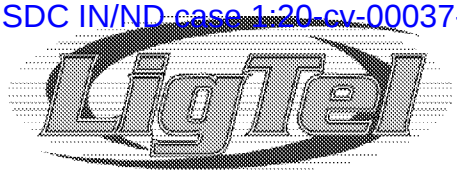
4.20 Software Installation

No non-company-supplied software is to be installed without written permission of the IT Manager. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. For these reasons, installation of non-company-supplied programs is strongly discouraged. If a certain program is required for his or her job function, the user should contact the IT Department to request permission.

4.21 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.



- Any other suspicious event that may impact the company's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

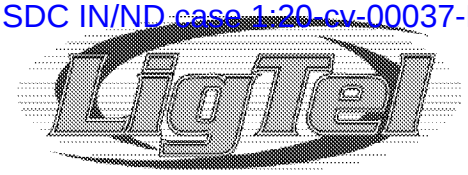
Blogging - The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging - A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing - A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access - Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media - Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

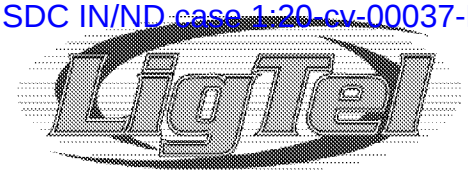


Cybersecurity Policies

Acceptable Use Polic	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 9 of 9

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Confidential Data Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 6

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

2.0 Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

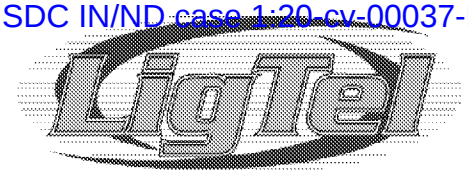
4.0 Policy

4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

4.1.1 Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.



4.1.2 Transmission

Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

4.1.3 Destruction

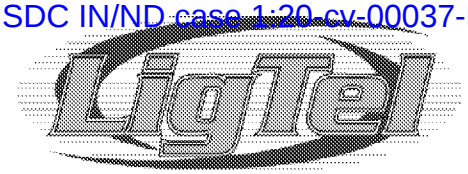
Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.

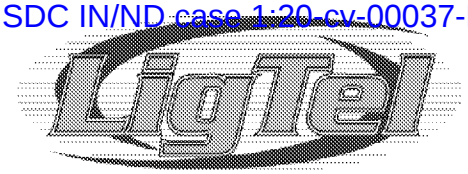


- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the company's outsourcing policy for additional guidance.

4.3 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted external to the company. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.
- Network Segmentation. Separating confidential data by network segmentation is strongly encouraged.
- Authentication. Strong passwords must be used for access to confidential data.
- Physical Security. Systems that contain confidential data should be reasonably secured.
- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.
- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- Emailing. Confidential data must not be emailed outside the company without the use of strong encryption.
- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information.
- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.

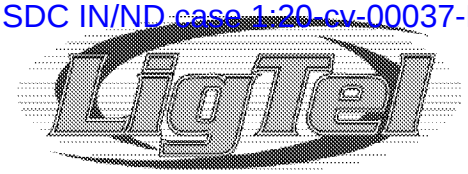


- Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- Confidential data must never be stored on non-company-provided machines (i.e., home computers).
- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

4.4 Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data (if company is closely held)
- Sales forecasts
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information



- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

4.5 Emergency Access to Data

A procedure for access to confidential and critical data during an emergency must be developed and documented. The company must establish a procedure for emergency access in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

The procedure should answer the following questions:

- What process must be followed to activate the emergency access procedure?
- What systems will it involve?
- In what situations should it be activated?
- Will it be activated automatically if certain conditions are met, or will it require human intervention? If so, who is authorized to make the decision to implement the procedure?
- Who will be involved in the process and what roles will they perform?

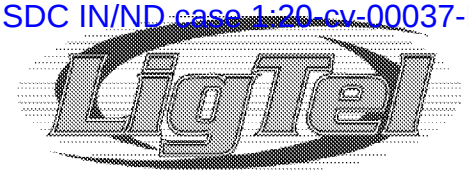
4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions



Cybersecurity Policies

Confidential Data Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 6 of 6

Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

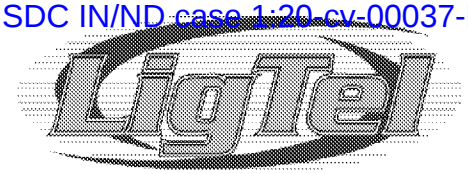
Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Two-Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Data Classification Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 5

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

Information assets are assets to the company just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, the company can take steps to ensure that data is treated appropriately.

2.0 Purpose

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

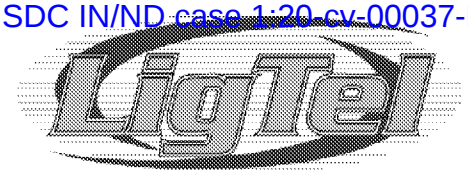
4.0 Policy

4.1 Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.



3. Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

4.2 Data Storage

The following guidelines apply to storage of the different types of company data.

4.2.1 Personal

There are no requirements for personal information.

4.2.2 Public

There are no requirements for public information.

4.2.3 Operational

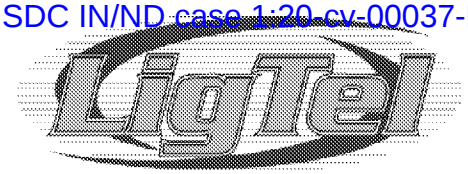
Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

4.2.4 Critical

Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

4.2.5 Confidential

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.



Cybersecurity Policies

Data Classification Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 3 of 5

4.3 Data Transmission

The following guidelines apply to transmission of the different types of company data.

4.3.1 Personal

There are no requirements for personal information.

4.3.2 Public

There are no requirements for public information.

4.3.3 Operational

No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

4.3.4 Critical

There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

4.3.5 Confidential

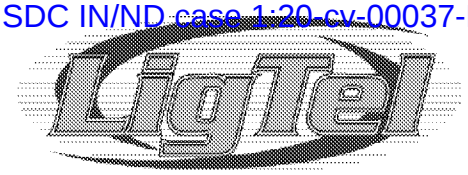
Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

4.4 Data Destruction

The following guidelines apply to the destruction of the different types of company data.

4.4.1 Personal

There are no requirements for personal information.



Data Classification Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 5

4.4.2 Public

There are no requirements for public information.

4.4.3 Operational

Cross-cut shredding is required for documents. Storage media should be appropriately sanitized/wiped or destroyed.

4.4.4 Critical

There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

4.4.5 Confidential

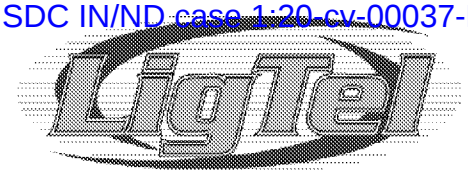
Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

4.5 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement



Cybersecurity Policies

Data Classification Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 5 of 5

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

Backup - To copy data to a second location, solely for the purpose of safe keeping of that data.

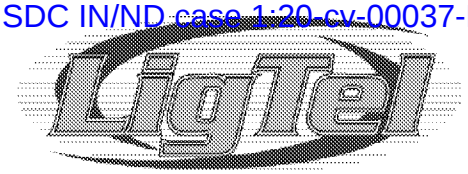
Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Two-Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Email Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 13

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the company's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail the company's usage guidelines for the email system. This policy will help the company reduce risk of an email-related security incident, foster good business communications both internal and external to the company, and provide for consistent and professional application of the company's email principles.

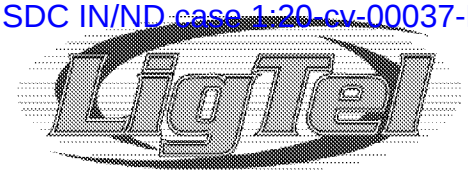
3.0 Scope

The scope of this policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network.

4.0 Policy

4.1 Proper Use of Company Email Systems

Users are asked to exercise common sense when sending or receiving email from company accounts. Additionally, the following applies to the proper use of the company email system.



Cybersecurity Policies

4.1.1 Sending Email

When using a company email account, email must be addressed and sent carefully. Users should keep in mind that the company loses any control of email once it is sent external to the company network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the company avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use and General Guidelines

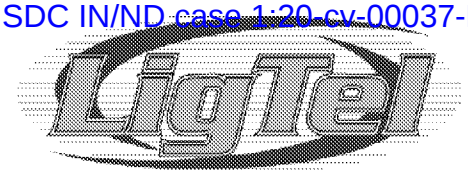
Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.
- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this policy.

4.1.3 Business Communications and Email

The company uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.



Additionally, users are asked to recognize that email sent from a company account reflects on the company, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature

Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of the individual user. Users are asked to keep any email signatures professional in nature; however the company does not place any restrictions on email signature content.

4.1.5 Auto-Responders

The company requires the use of an auto-responder if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

4.1.6 Mass Emailing

The company makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with the company's employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

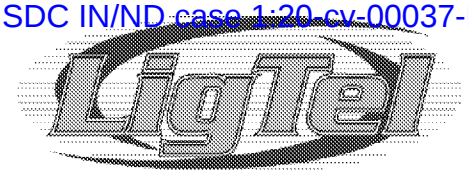
It is the company's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the company requires that email sent to more than twenty (20) recipients external to the company have the following characteristics:

1. The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.

2. The email must contain a subject line relevant to the content.

3. The email must contain contact information, including the full physical address, of the sender.

4. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.



Cybersecurity Policies

Email Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 13

Note that emails sent to company employees, existing customers, or persons who have already inquired about the company's services are exempt from the above requirements.

4.1.7 Opening Attachments

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments.
- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

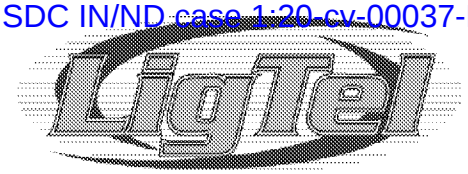
The company may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 Company Ownership of Email

Users should be advised that the company owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the company and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.



4.1.10 Contents of Received Emails

Users must understand that the company has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the company may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor.

4.1.11 Access to Email from Mobile Devices

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. The company permits users to access the company email system from a mobile device. Refer to the Mobile Device Policy for more information.

4.1.12 Email Regulations

Any specific regulations (industry, governmental, legal, etc.) relating to the company's use or retention of email communications must be listed here or appended to this policy.

4.2 External and/or Personal Email Accounts

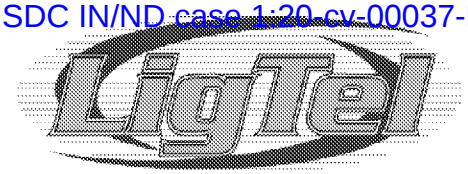
The company recognizes that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:

4.2.1 Use for Company Business

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account.

4.2.2 Access from the Company Network

Users are permitted to access external or personal email accounts from the corporate network, as long as such access uses no more than a trivial amount of the users' time and company resources.



4.2.3 Use for Personal Reasons

Users are strongly encouraged to use a non-company-provided (personal) email account for any non-business communications. Users must follow applicable policies regarding the access of non-company-provided accounts from the company network.

4.3 Confidential Data and Email

The following sections relate to confidential data and email:

4.3.1 Passwords

As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the IT Manager, the company may further secure email with certificates, two factor authentication, or another security mechanism.

4.3.2 Emailing Confidential Data

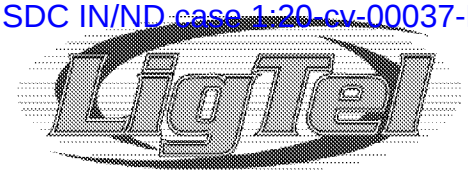
Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

The company requires that any email containing confidential information sent external to the company be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to the company. When in doubt, encryption should be used.

Further guidance on the treatment of confidential information exists in the company's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

4.4 Company Administration of Email

The company will use its best effort to administer the company's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.



Cybersecurity Policies

4.4.1 Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, the company will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the company's IT security. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the IT Manager.

4.4.2 Email Disclaimers

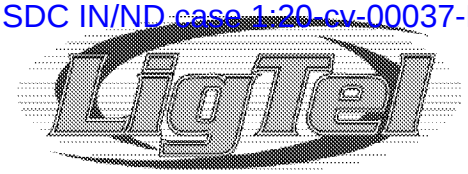
The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in the company's risk reduction efforts. The company requires the use of email disclaimers on every outgoing email, which must contain the following notices:

- The email is for the intended recipient only
- The email may contain private information
- If the email is received in error, the sender should be notified and any copies of the email destroyed
- Any unauthorized review, use, or disclosure of the contents is prohibited

An example of such a disclaimer is:

> *NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.*

The company should review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.



4.4.3 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the company to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another company policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

The company must note and document here any applicable regulations or statutes that apply to email deletion.

4.4.4 Retention and Backup

Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

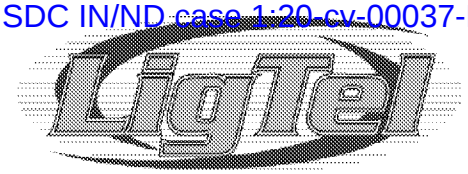
Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

4.4.5 Address Format

Email addresses must be constructed in a standard format in order to maintain consistency across the company. Some recommended formats are:

- Firstname.lastname@companydomain.com
- Firstinitial.lastname@companydomain.com
- Firstname lastname@companydomain.com
- FirstnameLastname@companydomain.com

The company can choose virtually any format, as long as it can be applied consistently throughout the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.



4.4.6 Email Aliases

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of company employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- sales@companydomain.com
- techsupport@companydomain.com
- pr@companydomain.com
- info@companydomain.com

The company requires the use of email aliases in all situations where an email address will be exposed to, or reachable by, the general public.

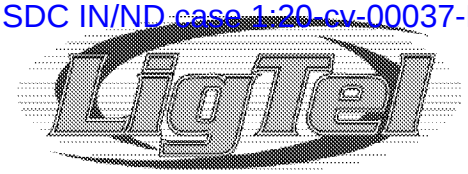
4.4.7 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive company email. Accounts will be set up at the time a new hire starts with the company, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

Accounts on the company email system will never be provided to non-employees of the company.

4.4.8 Account Termination

When a user leaves the company, or his or her email access is officially terminated for another reason, the company will disable the user's access to the account by password change, disabling the account, or another method. The company is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the company.



Email Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 10 of 13

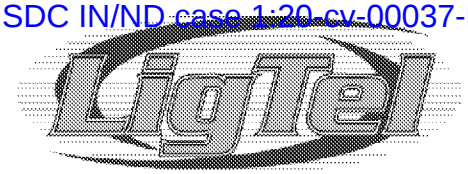
4.4.9 Storage Limits

As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IT Manager. Storage limits may vary by employee or position within the company.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

- Send any information that is illegal under applicable laws.
- Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of company executives in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.
- Send any emails that may cause embarrassment, damage to reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent the company's capabilities, business practices, warranties, pricing, or policies.
- Conduct non-company-related business.



The company may take steps to report and prosecute violations of this policy, in accordance with company standards and applicable laws.

4.5.1 Data Leakage

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the company's control of its data.

Unauthorized emailing of company data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from company systems.

The company may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IT Manager.

4.5.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The company asks that the user limit email attachments to 10Mb or less.

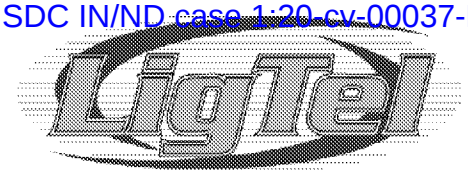
The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities. If any provision of this policy is found to be



unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

6.0 Definitions

Auto Responder - An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate - Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage - Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email - Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

Encryption - The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

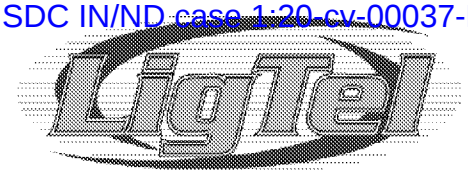
Mobile Device - A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Password - A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Spam - Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Smartphone - A mobile telephone that offers additional applications, such as PDA functions and email.

Two Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

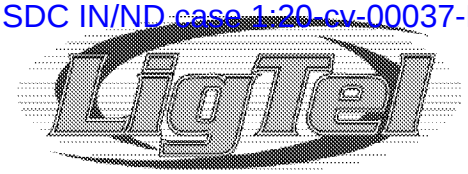


Cybersecurity Policies

Email Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 13 of 13

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Mobile Device Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 5

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify company standards for the use and security of mobile devices.

3.0 Scope

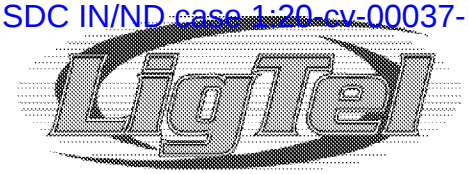
This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with company data.

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The company should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.
- Mobile devices should be kept out of sight when not in use.



- Care should be given when using or transporting mobile devices in busy areas.
- As a general rule, mobile devices should not be stored in cars. If the situation leaves no other viable alternatives, the device must be secured within the vehicle.
- The company should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.
- The company should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify the company's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

Whole disk encryption is required. Laptops must require a username and password or biometrics for login.

4.2.2 Smartphones/Tablets

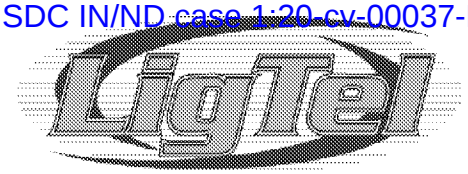
Use of encryption is not required on smartphones and tablets but it is encouraged if data stored on the device is especially sensitive. Smartphones and tablets must require a password for login.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Encryption is required on these devices when they contain company information.

4.2.4 Portable Media Players

No company data can be stored on personal media players.



4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the company.

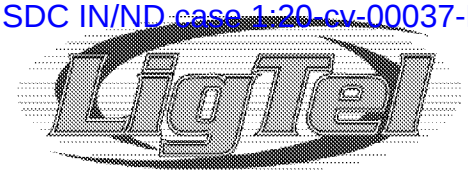
4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.
- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.
- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.
- Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

4.5 Audits

The company must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on a periodic basis.



Mobile Device Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 5

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices - A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

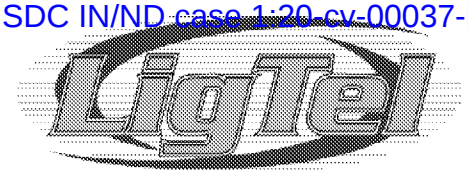
Mobile Storage Media - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password - A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA - Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player - A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone - A mobile telephone that offers additional applications, such as PDA functions and email.

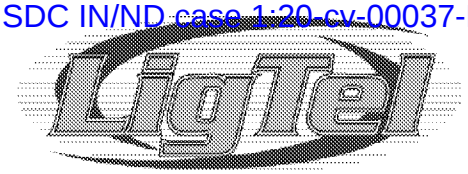


Cybersecurity Policies

Mobile Device Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 5 of 5

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Password Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope

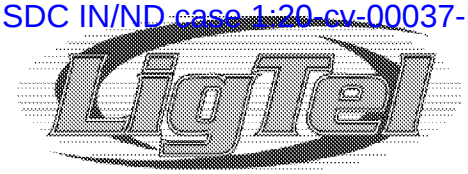
This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction

The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower case characters



- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

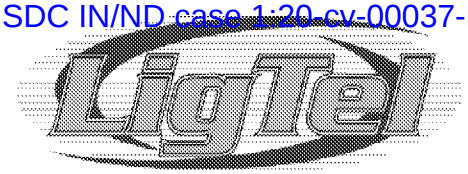
Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured
- Users must not check the "save password" box when authenticating to applications
- Users must not use the same password for different systems and/or accounts
- Users must not send passwords via email
- Users must not re-use the last 3 passwords



Cybersecurity Policies

4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Manager. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Manager will request that the user, or users, change all his or her passwords.

4.5 Applicability of Other Policies

This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

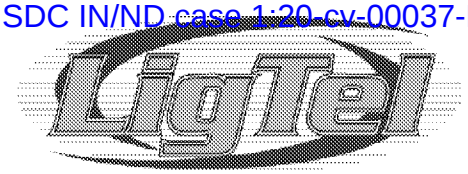
5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

Password - A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.



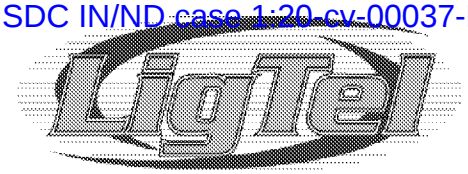
Cybersecurity Policies

Password Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 4

Two Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Remote Access Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 3

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the company's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

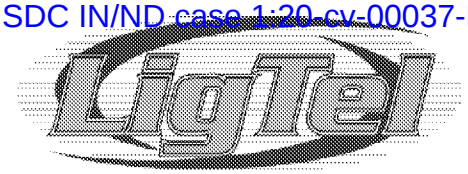
The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with company-provided or non-company-provided equipment.

4.0 Policy

4.1 Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of the IT Manager.



Cybersecurity Policies

- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the IT Manager.
- Use of non-company-provided remote access software.
- Split Tunneling to connect to an insecure network in order to bypass security restrictions.

4.2 Use of non-company-provided Machines

Accessing the corporate network through home or public machines presents a security risk, as the company cannot completely control the security of the system accessing the network. No non-company-provided computers are allowed to access the corporate network for any reason.

4.3 Client Software

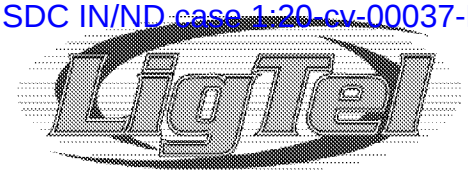
The company may or may not supply users with remote access client software or VPN software, depending on the business need for accessing corporate systems remotely. Unless provided by default, users requiring remote access should document their needs in a request to the IT Manager, who will determine if the request is feasible from a business and technology perspective, and will be responsible for deploying any necessary remote access in such a manner that is consistent with the company's security strategy. At a minimum, the software will include data encryption with industry-standard encryption algorithms. Additional security options, such as a bundled client firewall, can be included at the discretion of the IT Manager.

4.4 Network Access

The company will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform his or her job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections.

4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the company's network must be timed out after 1 hour of inactivity.



Cybersecurity Policies

Remote Access Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 3 of 3

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Modem - A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access - The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

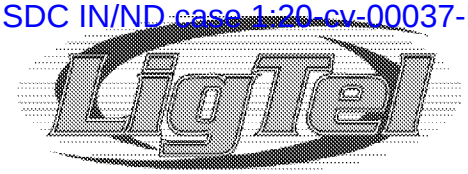
Split Tunneling - A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout - A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 9/14/2017



Cybersecurity Policies

Retention Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

LigTel Communications is hereinafter referred to as "the company."

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organization.

2.0 Purpose

The purpose of this policy is to specify the company's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

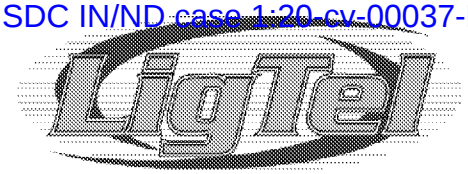
Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Reasons for Data Retention

The company does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:



Cybersecurity Policies

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of company data.

Personal There are no retention requirements for personal data. In fact, the company encourages that it be deleted or destroyed when it is no longer needed.

Public There are no retention requirements for public data beyond what the owner of the data desires.

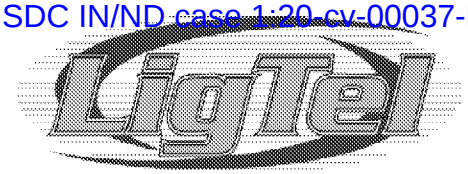
Operational Most company data will fall in this category. Operational data must be retained for 1 year.

Critical Critical data must be retained for 2 years.

Confidential Confidential data must be retained for 2 years.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.



Cybersecurity Policies

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's executive team.

The company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy.

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

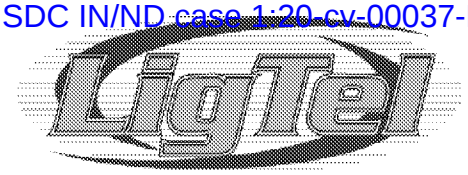
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Backup - To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption - The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key - An alphanumeric series of characters that enables data to be encrypted and decrypted.



Cybersecurity Policies

Retention Policy	Created: 9/14/2017
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 4 of 4

7.0 Revision History

Revision 1.0, 9/14/2017